Concepts and Trends in Information Survivability

CERT® Centers
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Networked Systems Survivability

Who Is Saying This?

"Security models should be easy for developers to understand and build into their applications."

"Our products should emphasize security right out of the box."

"As software has become ever more complex, interdependent and interconnected, our reputation as a company has in turn become more vulnerable."

"So now, when we face a choice between adding features and resolving security issues, we need to choose security."

"Eventually, our software should be so fundamentally secure that customers never even worry about it."

Networked Systems Survivability

Attack Trends

Increased automation, speed of attack tools

Increased attack tool sophistication

Faster discovery of vulnerabilities

Increasing permeability of firewalls

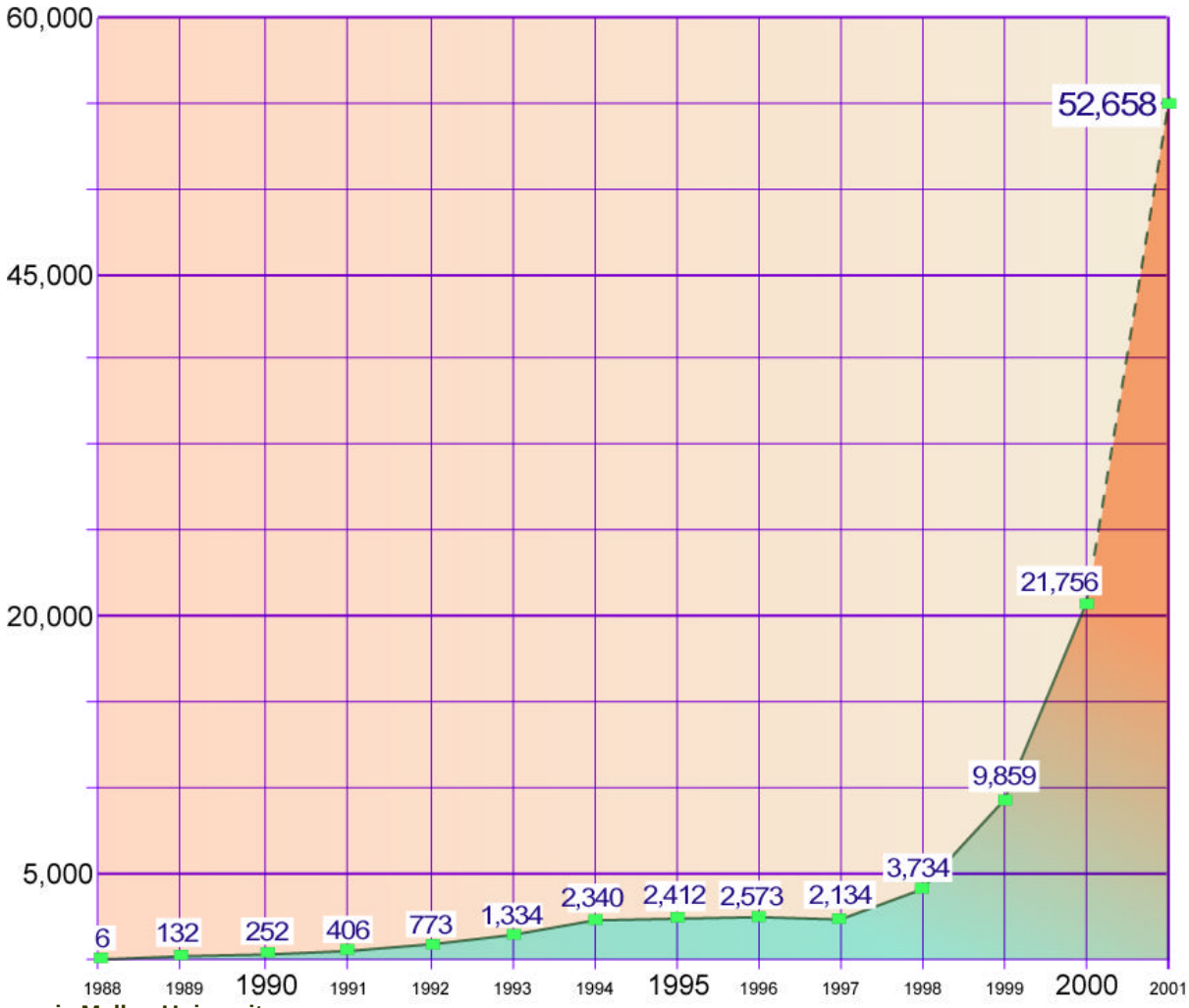
Increasing asymmetric threat

Increasing threat from infrastructure attacks

http://www.cert.org/archive/pdf/attack_trends.pdf

Networked Systems Survivability

Growth in Number of Incidents Reported to the CERT/CC



Attack Impacts

Loss/compromise of sensitive data

System downtime; lost productivity

System damage

Financial loss

Loss of reputation, customer/collaborator confidence

Other organizations' systems affected

Information Survivability

Focuses on sustaining the mission in the face of an ongoing attack; requires an enterprise-wide perspective

Depends on the ability of networks and systems to provide continuity of essential services, albeit degraded, in the presence of attacks, failures, or accidents

Requires that only the critical assets need the highest level of protection

Complements current risk management approaches that are part of an organization's business practices

Includes (but is broader than) traditional information security

Networked Systems Survivability

Shifts in Thinking

Central to Global

Bounded to Unbounded

Insular to Networked

Predictable to Asynchronous

Single Responsibility to Shared

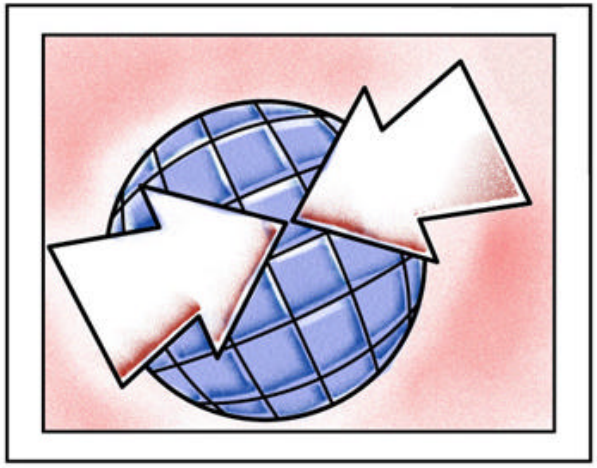
Overhead to Essential

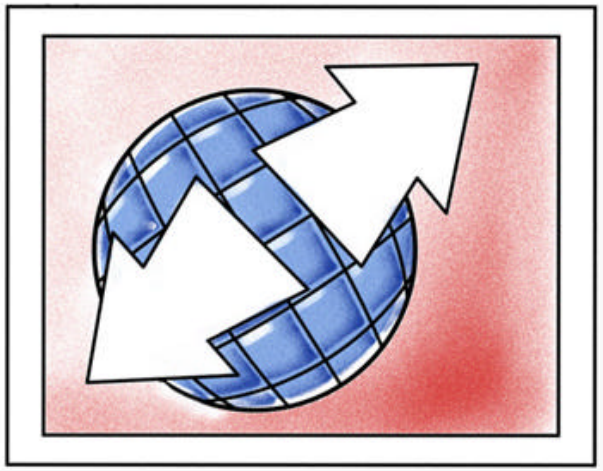
Security to Survivability

Networked Systems Survivability

Shift in Thinking -1

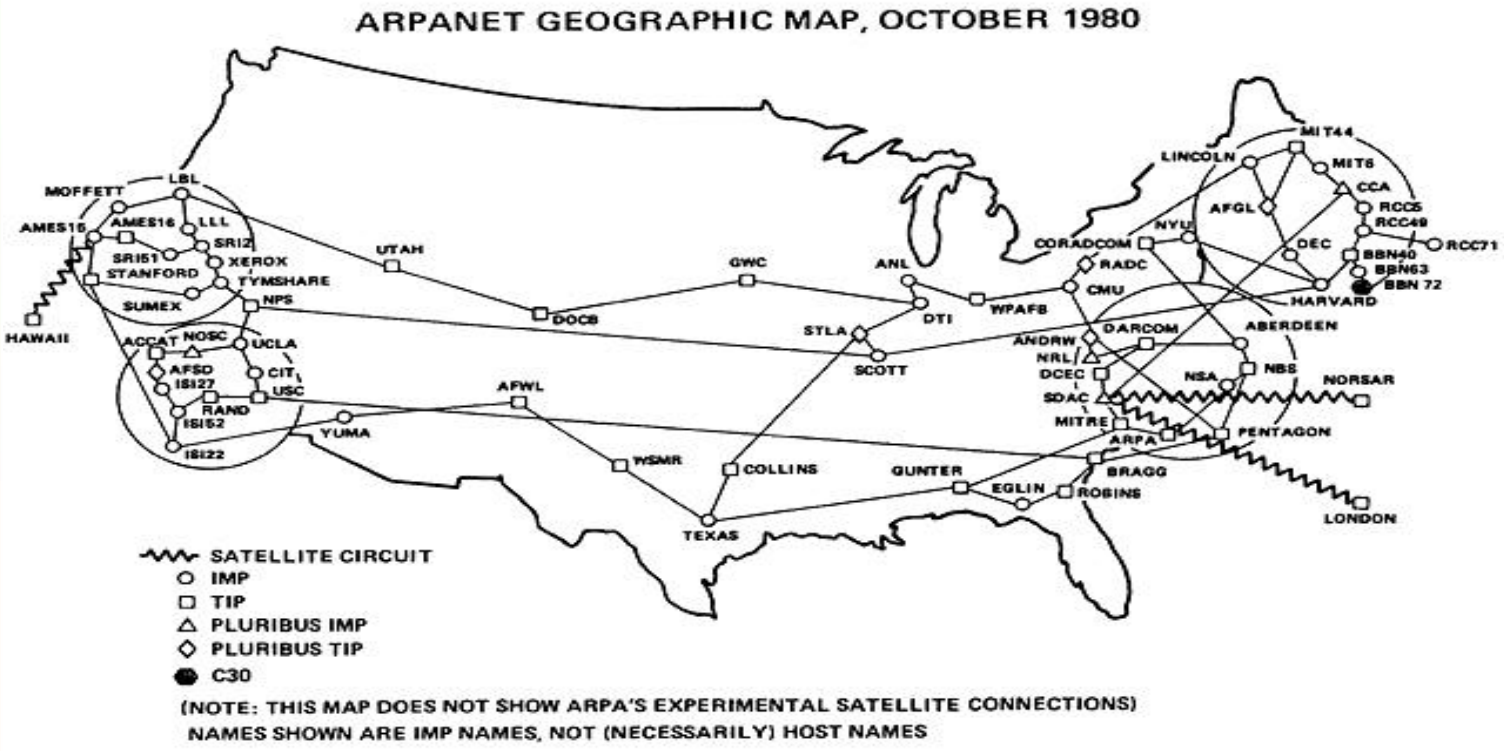
Centrally networked environment (under organizational control, full visibility) → to → Globally networked environment (unbounded, no central control, limited visibility)



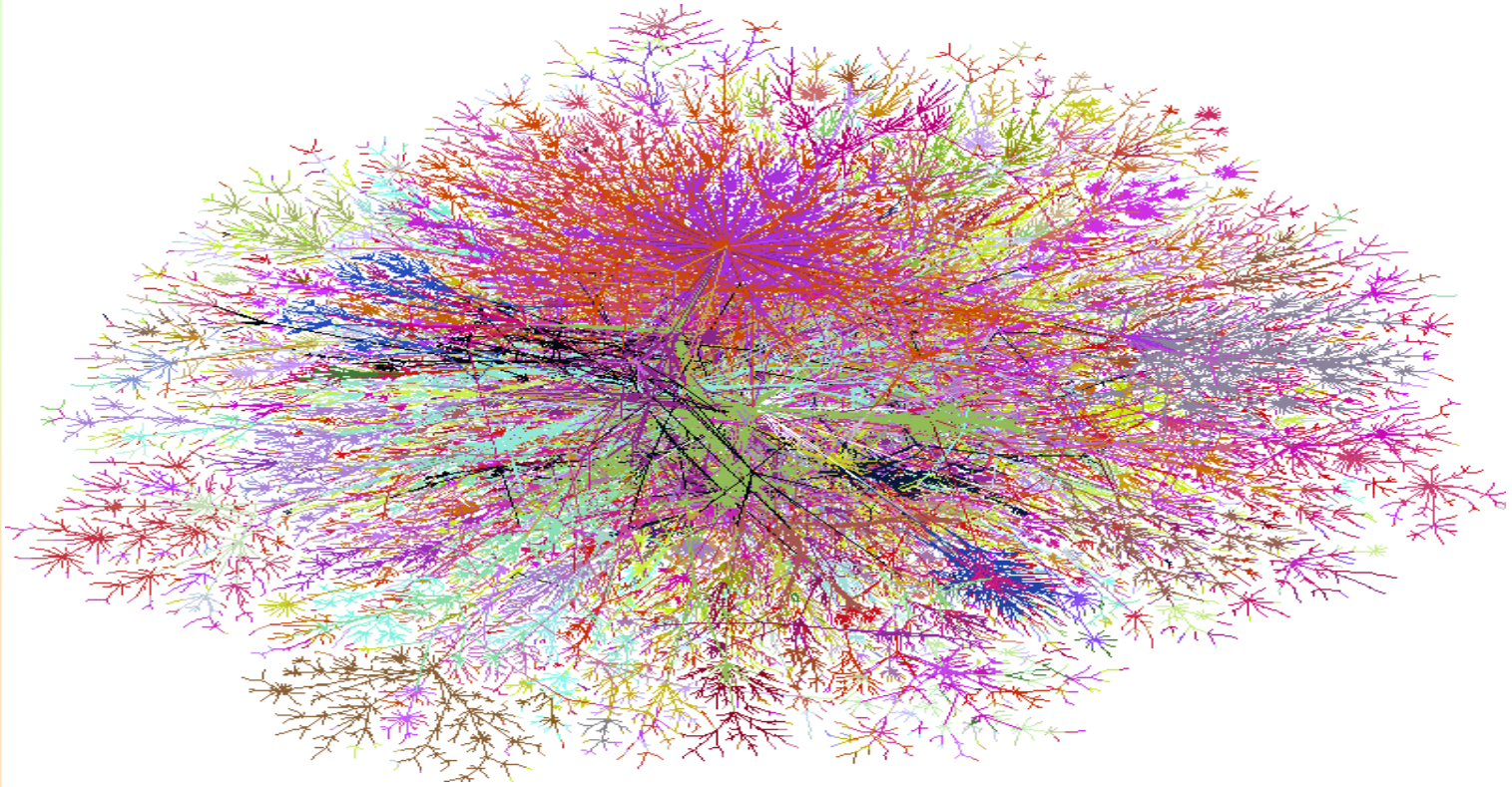


Networked Systems Survivability

The Old 'Net



The New 'Net



Source: http://cm.bell-labs.com/who/ches/map/gallery/index.html

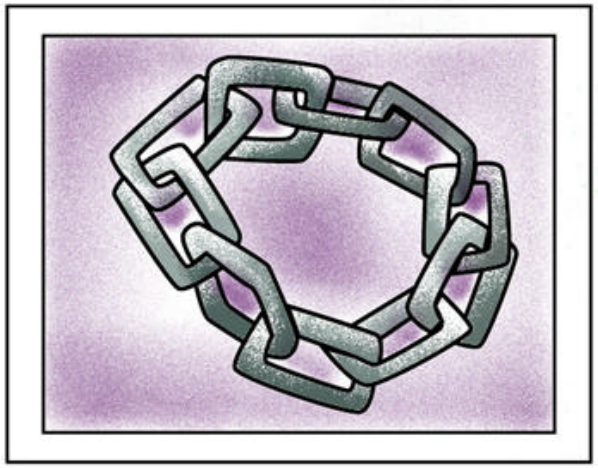
Networked Systems Survivability

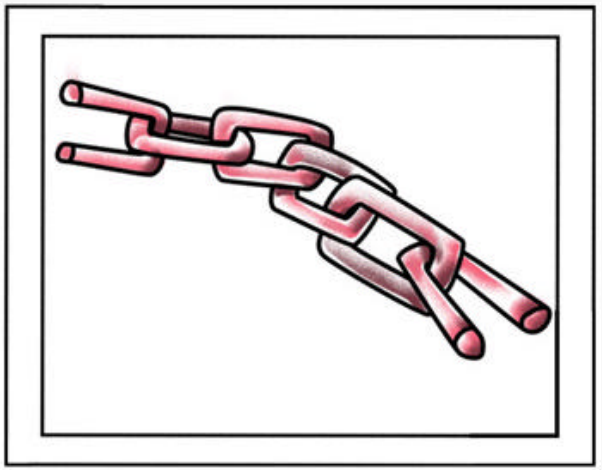
Shift in Thinking -2

Bounded (discrete, fixed, complete, done, known)

to →

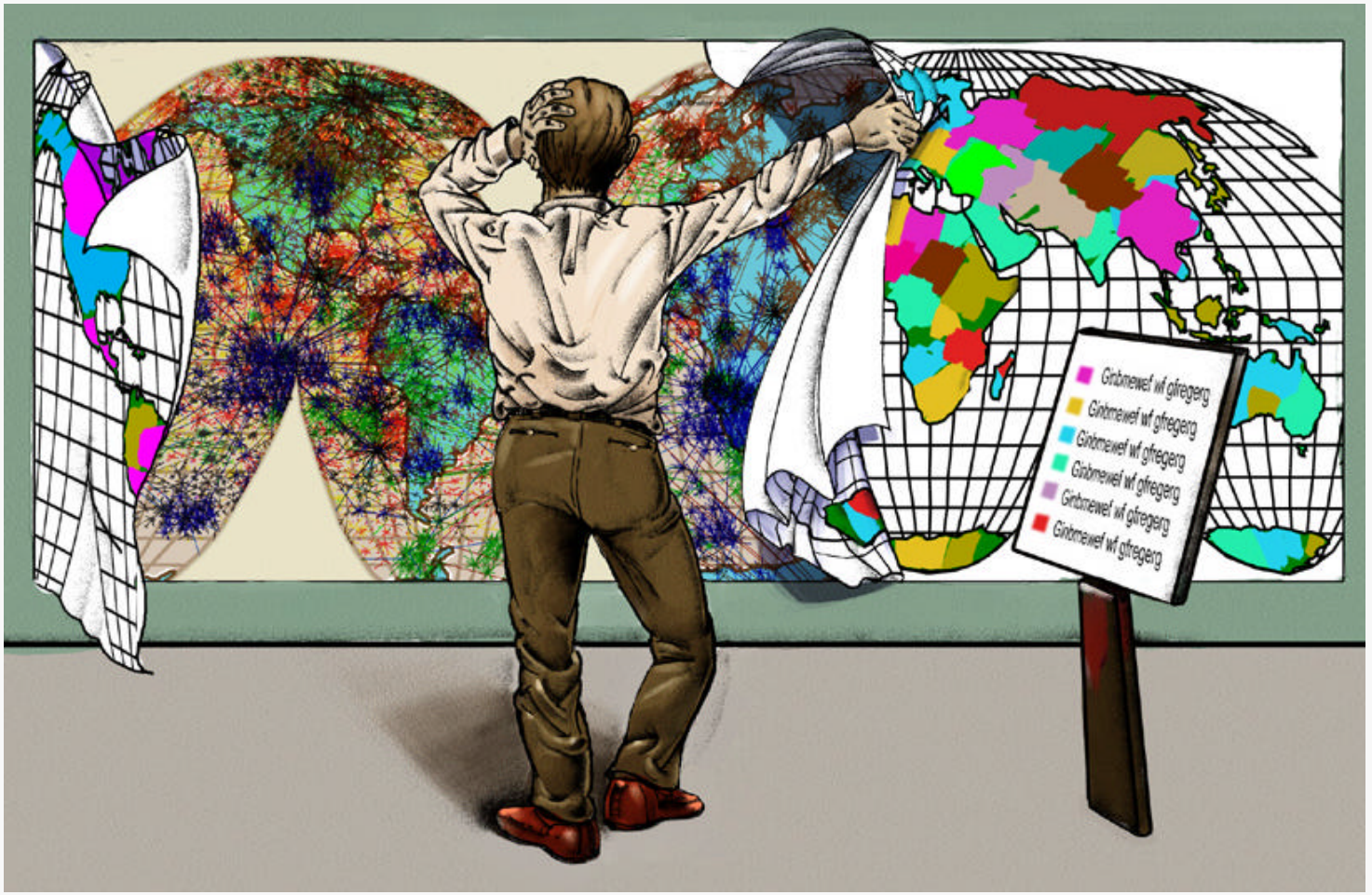
Unbounded (no known end point or perimeter, continuously evolving)





Networked Systems Survivability

Bounded to Unbounded



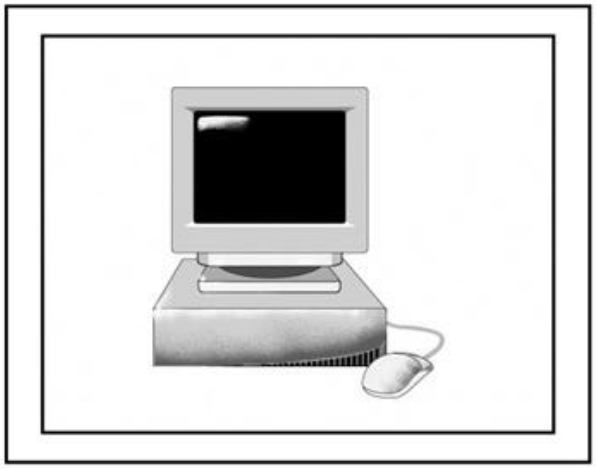
Networked Systems Survivability

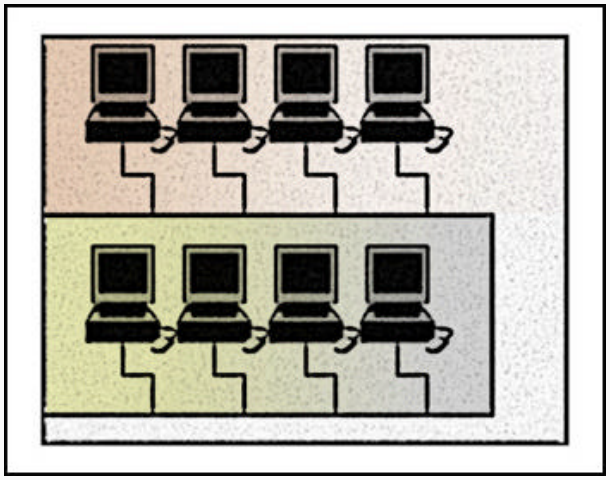
Shift in Thinking -3

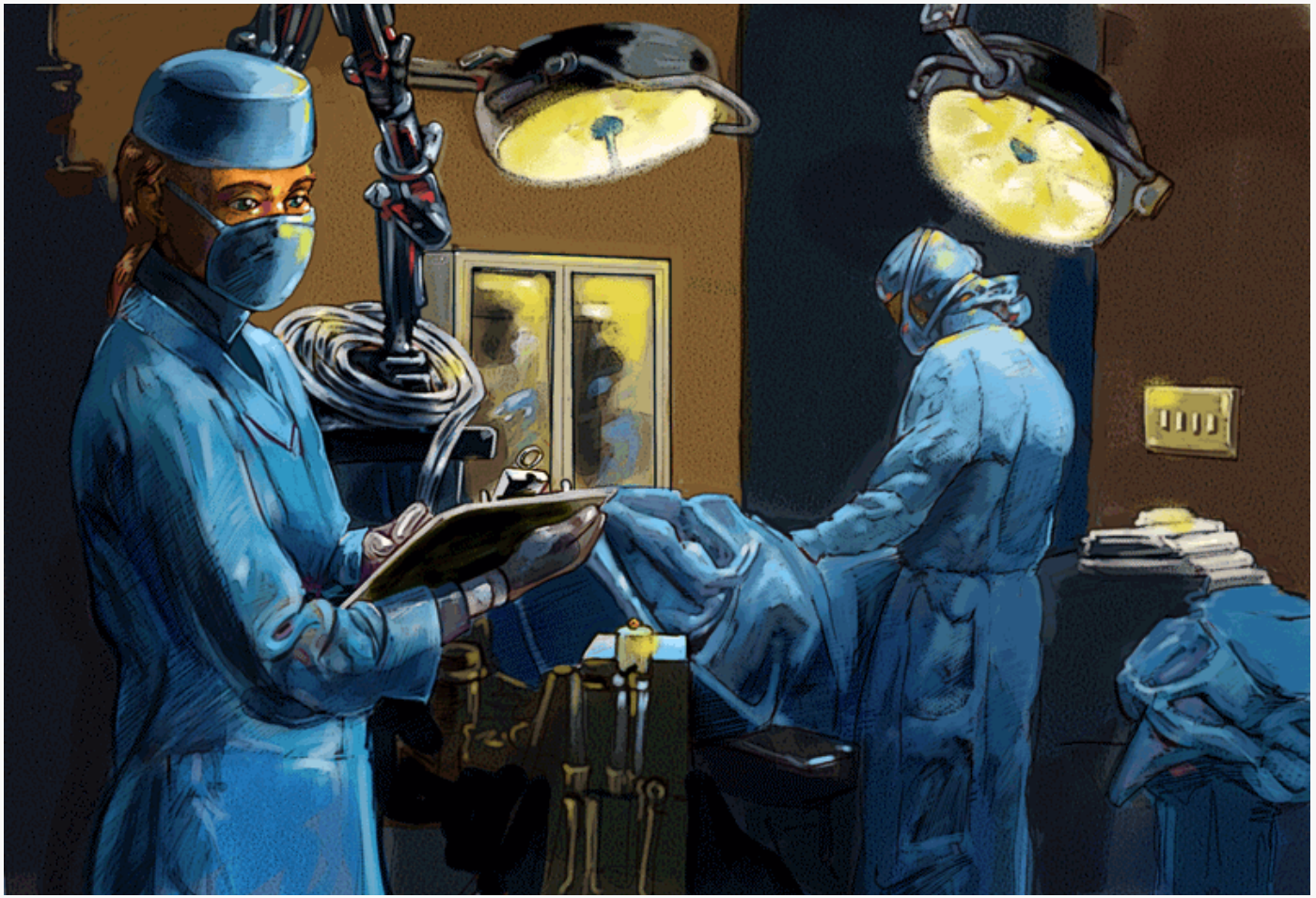
Insular, fortress-like, hierarchical, independent; clear distinction between insiders and outsiders

to →

Networked, connected, interdependent; decreasing distinction between insiders and outsiders





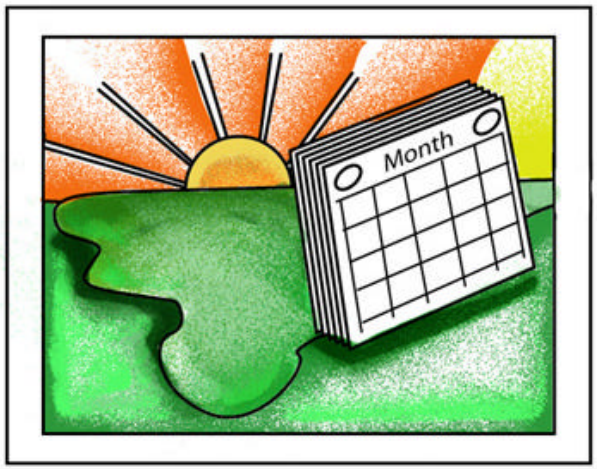


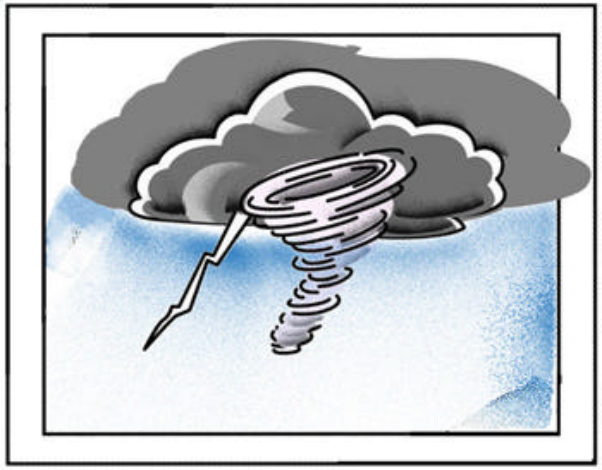
Shift in Thinking -4

Processing events happen in predictable, prescribed sequences and patterns

to →

Events often occur independent of time sequence; asynchronously, unpredictably





Networked Systems Survivability

Coast Guard

Internal Oracle database compromised in 1997

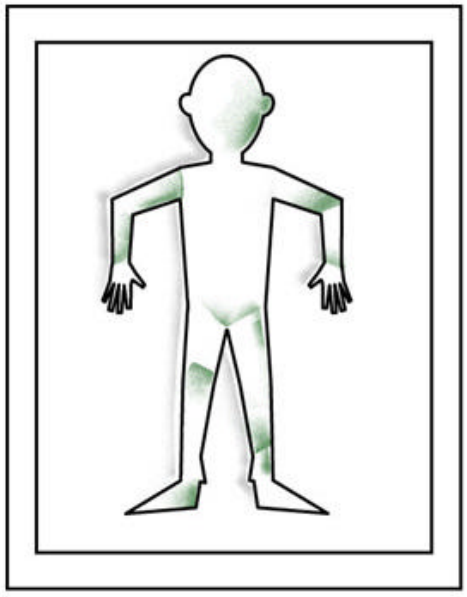
- Crashed server leads to immediate recognition. Took 115 Coast Guard employees more than 1800 hours to restore lost data (manually enter personnel data).
- System down time—36 hours

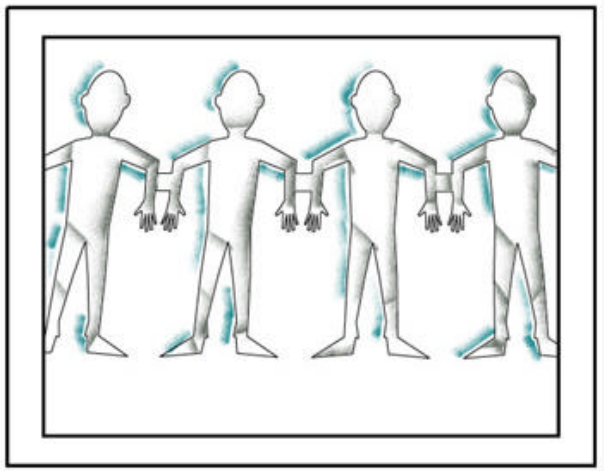
This was caused by a disgruntled employee who had left the Coast Guard.

Source: Computerworld 7/20/98

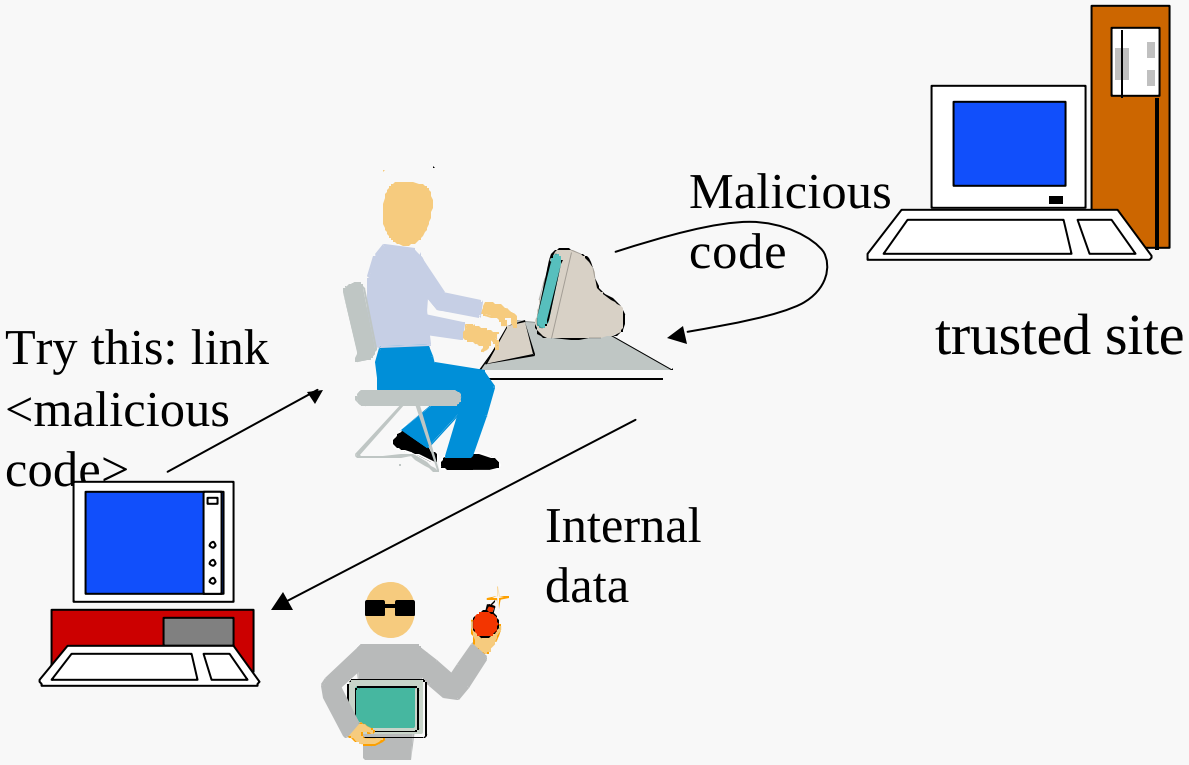
Shift in Thinking -5

Single point of known responsibility to correct failures → to → Shared, sometimes unknown, responsibility





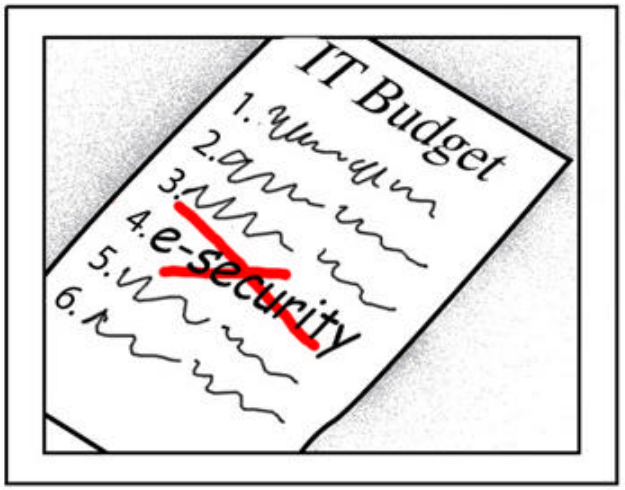
Cross-Site Scripting

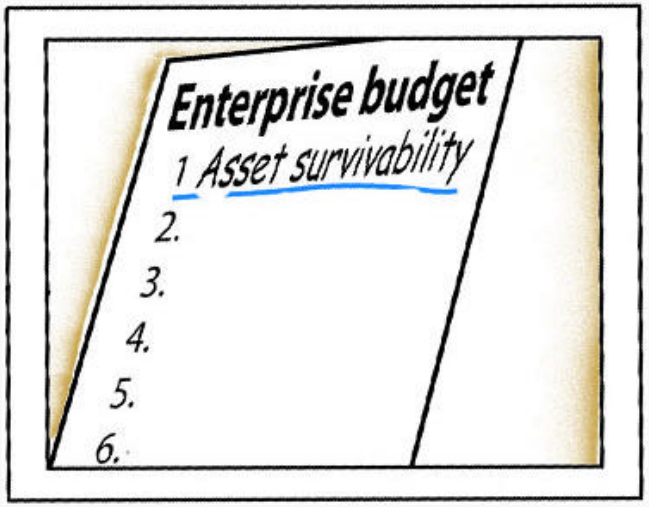


http://ts.gov/script.cgi?id=<script> evil </script>

Shift in Thinking -6

Security viewed as an overhead activity → to → Survivability viewed as essential to the business





Networked Systems Survivability

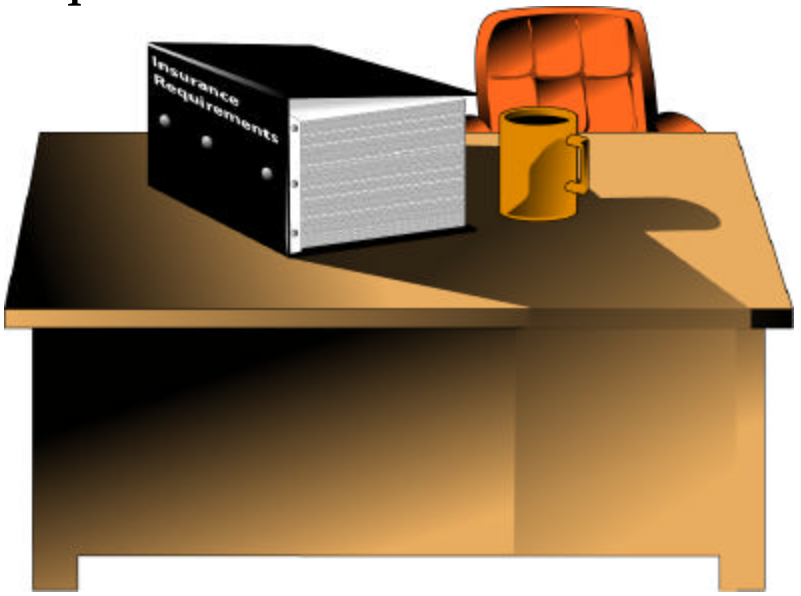
IA Regulations and Standards

National legislation (privacy, etc.)

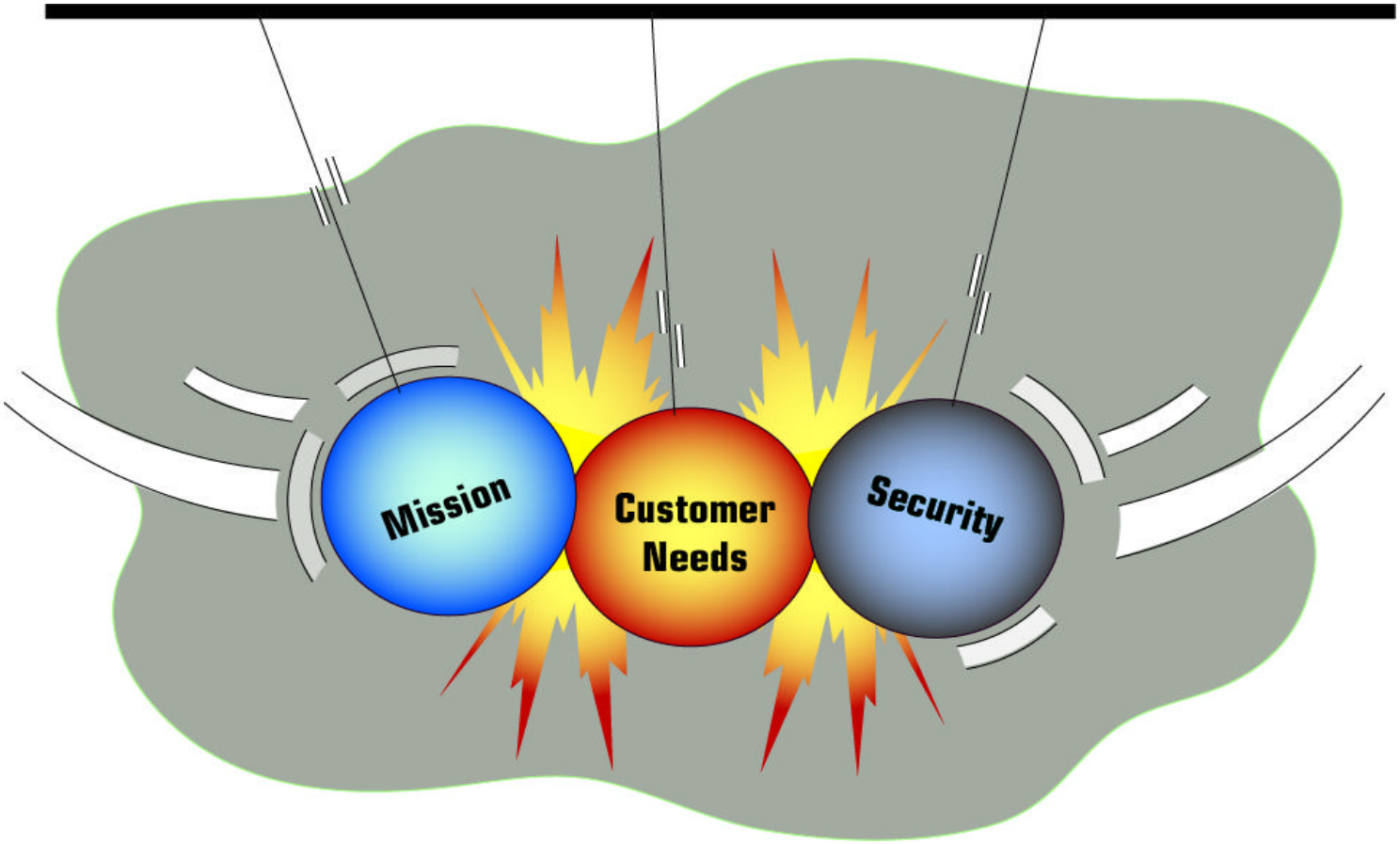
Insurance industry requirements

Consumer demand

E-torts and e-pacts



Collision of Mission, Customer Needs, and Security

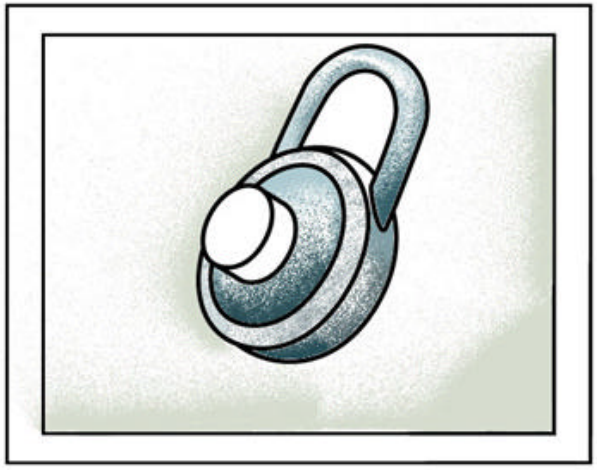


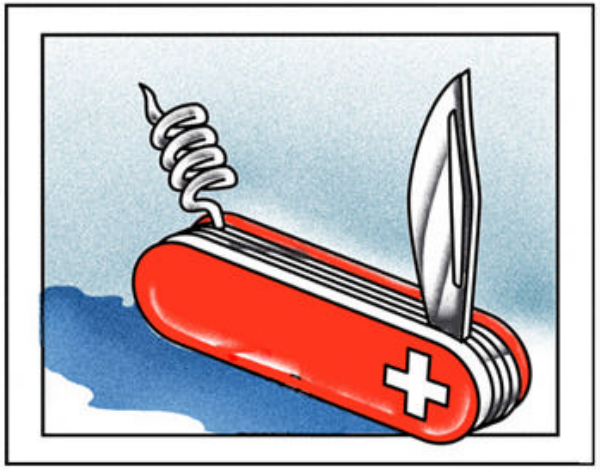
Shift in Thinking -7

Security as a narrow technical specialty accessible only to experts; protection of specific components

to →

Survivability as a risk management perspective requiring involvement of the whole organization; survival of mission





How Are You Managing E-risks Now in Your Organization?

E-policies, governance

Critical information assets

Who to involve

Management controls

Sustain survivability

Candidate Elements of the Solution

Shift your thinking

Ask the right questions

Understand what your risks are in relation to your organization's mission and its key assets (risk assessment)

Enforce an information security policy that reflects your business goals

Vote with your dollars (when purchasing vendor products)

Keep security and survivability issues visible

Deploy a layered security architecture (diversity, distribution)

Networked Systems Survivability

Layered Security Architecture

Eliminate known vulnerabilities; apply patches; deploy secure configurations

Characterize and regularly check integrity of critical assets

Use firewalls, access control, user authentication, and encryption technologies

Use network and system monitoring tools including intrusion detection

Periodically conduct vulnerability and penetration testing; act on the results

Use virus detection and eradication software; keep signatures up to date

Conduct ongoing training for users, administrators, and managers

Networked Systems Survivability

Life-cycle Activities -1

Life-Cycle Activity	Key Survivability Elements	Example
Mission definition	Analysis of mission criticality and consequences of failure	Estimation of cost impact of denial-of-service attacks
Concept of operations	Definition of system capabilities in adverse environments	Enumeration of critical mission functions that must withstand attacks
Project planning	Integration of survivability into life-cycle activities	Identification of defensive coding techniques for implementation
Requirements definition	Definition of survivability requirements from mission perspective	Definition of access requirements for critical system assets during attacks
System specification	Specification of essential service and intrusion scenarios	Definition of steps that compose critical system transactions

From: Life-cycle Activities and Corresponding Survivability Elements Table in *Annuals of S/W Engr.* (Vol.11, 2001, pp 45-78)

Networked Systems Survivability

Life-cycle Activities -2

Life-Cycle Activity	Key Survivability Elements	Example
System architecture	Integration of survivability strategies into architecture definition	Creation of network facilities for replication of critical data assets
System design	Development and verification of survivability strategies	Verification of data-encryption algorithms for correctness
System implementation	Application of survivability coding and implementation techniques	Definition of methods to avoid buffer overflow vulnerabilities
System testing	Treatment of intruders as users in testing and certification	Addition of intrusion usage to usage models for statistical testing; use of independent verification and validation
System evolution	Improvement of survivability to prevent degradation over time	Redefinition of architecture in response to changing threat environment

From: Life-cycle Activities and Corresponding Survivability Elements Table in *Annuals of S/W Engr.* (Vol.11, 2001, pp 45-78)

Six Tips for Selling Security

Establish Need Before Cost

Hit 'Em with Numbers

Use Others' Losses to Your Advantage

Put It in Legal Terms

Keep It Simple

— Field, Tom. "Protection Money." CIO Magazine. October 1, 2000. Available at http://www2.cio.com/archive/100100_money_content.html

Networked Systems Survivability

Questions To Consider

What are your most important assets necessary to fulfill your mission, in a timely manner, in the presence of attacks, failures, or accidents?

What are the highest impact threats to those assets? Under what circumstances are they most at risk?

What are the key survivability concerns with respect to those assets?

Networked Systems Survivability

Next Steps to Consider

Address the questions on the previous slide

Ensure this perspective is promulgated throughout the organization (starting with your direct reports)

Ensure your IT organization and administration staff understand this sufficiently to make it operational, over time

What questions would you ask in order to determine where your organization is with respect to each of the 7 shifts in thinking?

Networked Systems Survivability

For More Information

CERT/CC
http://www.cert.org/
CERT/CC security practices
http://www.cert.org/security-improvement/
CERT/CC training
http://www.cert.org/nav/index_gold.html
OCTAVE℠
http://www.cert.org/octave/
CERT/CC survivability research
http://www.cert.org/nav/index_purple.html
ISAlliance
http://www.isalliance.org

Operationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.